The Advanced Encryption Standard (AES)

The Third Conference

Bill Burr, Computer Security Division,
Information Technology Laboratory,
National Institute of Standards and Technology

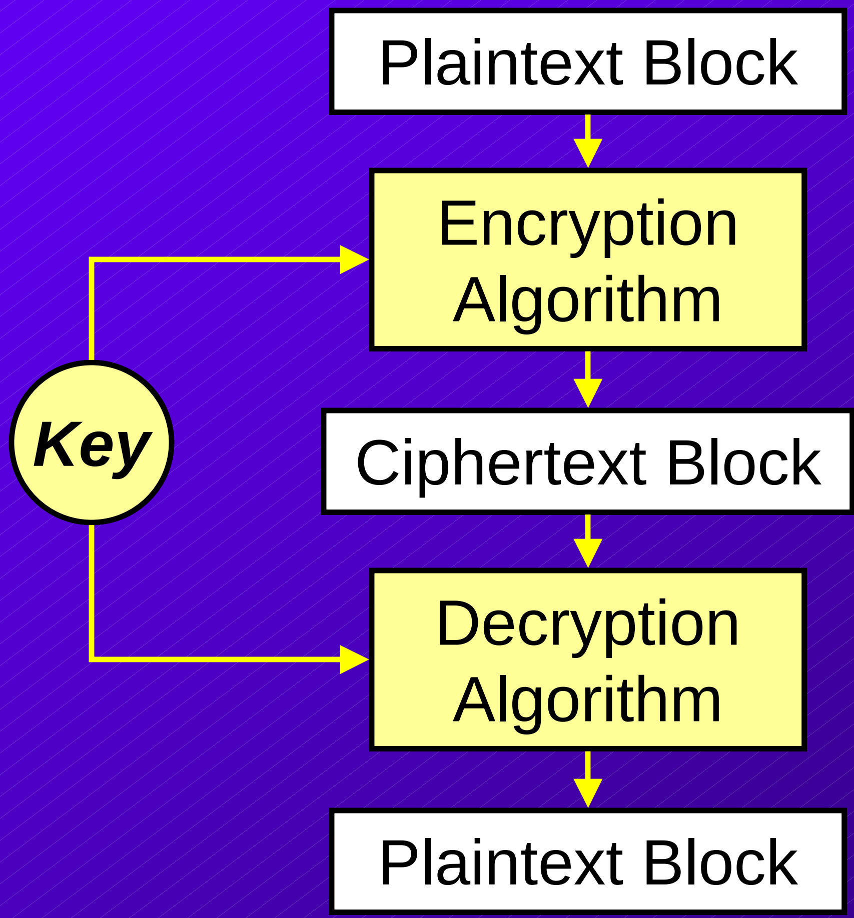
william.burr@nist.gov
http://www.nist.gov/aes

Today's Briefing

- AES Goals
- Past History
- Current Status after AES3
- Future Plans
- New Issues

NIST

Symmetric Key Block Cipher



AES Goals

- Provide a highly secure standard, with wide confidence, to protect sensitive information
- Replace aging Data Encryption Standard (DES)
- Secure enough for 20-30+ years
  - Larger block size (128-bit)
  - Larger, variable key sizes (min. 128-, 192-, 256-bit)
- Efficient in many environments
- Available world-wide royalty-free

AES Timeline - Past Milestones

January 1997 - Call for comments on Requirements & Evaluation Criteria

Sept. 1997 - Call for Candidate Algorithms

Aug. 1998 - NIST announces 15 candidates, begins Round 1 of analysis

March 1999 - Second AES Conference

April 1999 - Close of Round 1

NIST's Selection of Finalists

- Goal: Select **five** finalists to focus analysis
- Evaluated 56+ sets of public comments, 28 papers from AES2, & other data
- Based evaluations on these criteria:
  1. **Security**
  2. **Cost** (efficiency / intellectual property)
  3. **Flexibility**

NIST

AES Finalists

August 9, 1999 - Announcement of finalists;
began Round 2 analysis

MARS

RC6

Rijndael

Serpent

Twofish

AES 3 Conference

- New York City April 13 - 14
  – followed Fast Software Encryption conf.
- About 250 Participants
  – many of the world’s leading cryptographers
- 25 papers presented
  – plus rump session
- Algorithm submitters’ final summaries

NIST

AES 3 Papers

- Hardware evaluations
  - FPGA 3 papers
  - ASIC 3 papers
- Platform-specific evaluations
  - 5 papers

    64-bit platforms: PS-RISC, Alpha, IA-64

    high end DSPs

    high end smart cards

    Pentium in assembly & with MMX

NIST

AES 3 Papers

- Survey papers
  - 4 papers
    - Java (2), C on different platforms, one general summary of all results to date
- Cryptanalysis
  - 5 reduced round attacks
    - MARS (2)
    - Serpent
    - Rijndael (2)
  - 1 general properties (Rijndael)

AES 3 Papers

- Miscellaneous
  - future resiliency
  - effect of multiple winners
  - implementation tricks for Serpent

New Platforms

- Hardware
  – Serpant & Rijndael fastest, MARS slowest
- 64-bit architectures
  – Alpha Rijndael & Twofish fastest
  – IA-64 & PA RISC Rijndael fastest
- Signal Processor (TMS320C6201)
  – Twofish fastest, Serpent slowest
  – faster than Pentium (same clock)

NIST

MARS

- Proposed by IBM team
- Innovative, heterogeneous structure
  - outer wrapper of 16 mixing rounds
    - doesn't use key
  - inner core of 16 rounds
    - multiplies, shifts and substitutions
- Large security margin
  - claims high resilience against new attacks
  - complex, not easy to analyze

NIST

MARS

- Fast on 32-bit platforms
  - uses multiply instruction & circular shifts
- Relatively slow on 8 & 64 bit platforms
- Last in hardware
  - performance & area
- Poor key agility
  - large RAM requirements

RC6

- USA - RSA Security
- Simple / elegant
  - simple compact code
- Arguably well analyzed & understood
  - based on RC5
- Limited “security margin”
  - could easily be changed
- Allows parameterized rounds, key sizes, and word sizes

RC6

- Very fast on 32-bit platforms
  – uses multiply instruction & circular shifts
- Not so fast on other platforms
  – tailored to 32-bit instructions
    slows down on 64-bit platforms
- Fast key setup
  – reasonable key agility
- Indifferent hardware performance
- Suitability for low-end smart cards???

Rijndael

- Belgium
- 4 x 4 byte matrix structure
  – simple byte/matrix operations
- More rounds for larger keys
- Different encryption & decryption
  – Encryption a little faster than decryption
  – can't share same code

NIST

Rijndael

- Arguments about security margin?
  - is more analysis needed?
- Excellent performance on all platforms
- Fastest algorithm (i.e. low latency) for feedback mode in hardware
- Low RAM and ROM requirements
- Fast key setup
- Good potential for parallelism

Serpent

- UK, Israel & Norway team
- Large security margin (32 rounds)
- Simple structure
  - substitution & XOR
    - no multiply or data dependent shifts
  - arguably simplicity means well analyzed
- Low RAM and ROM requirements

Serpent

- Lowest software speed (most platforms)
  - not bad on 64-bit platforms
  - not bad for short blocks
  - recent improvements in software implementations
- Excellent key agility
- Well suited to hardware pipelining
  - fastest algorithm for nonfeedback modes

NIST

Twofish

- USA - Counterpane et al
- Key dependent S-boxes
- Large security margin
  – strongest round function?
- Complex
  – how well analyzed?

key separation property

has there been enough time?

Twofish

- Very fast across platforms
  - software & hardware
  - good key agility
- Low RAM and ROM requirements
- Flexible - can accommodate many time/space tradeoffs

AES Fundamental Operations

	Mars	RC6	Rijndael	Serpent	Twofish
Table- Lookup (Table Size)	8/ 9 to 32 (2,048 bytes)	none (0 bytes)	8 to 8 (256 bytes)	none (0 bytes)	two 8 to 8 (512 bytes)
Bitwise Boolean	XOR	XOR	XOR	XOR, AND, OR	XOR
Shift or Rotate Operation	Variable	Variable		Fixed	Fixed
Multiplication mod 2^{32}	X	X			
Addition mod 2^{32}	X	X			X
Multiplication GF(2^8)			X		X
Bitwise Permutation				standard mode	
Linear Transformation	X			X	

Tom Messerges, Motorola Labs

NIST

AES 3 Issues

- Security of algorithms
- Number of winners
- Intellectual Property
- Hardware
- Key agility
- New modes of operation
- Recommended key size

NIST

Security of Algorithms

- Security is most important factor
  - Each submitter thinks that his algorithm is most secure, or that it's a wash
  - No candidate is apparently weak
- More analysis was presented
  - no candidate really hurt
  - never enough analysis
- Analysis is slow work, but
- Need to make a choice soon

Single vs. Multiple Winners

- Two papers in favor
- Overwhelming sentiment at conference for a single winner:
  – twice the chance for IP problems
  – don't want to have to build two
  – better to "toss a coin" than have 2 or more
- Backup algorithm may be OK
  – some folks don't even like that
  – disaster strategy

NIST

Intellectual Property

- "IP attack" a more immediate concern than cryptanalytic attack
  - IP attack less likely with time
- Multiple winners makes the problem worse, not better
  - everybody will have to implement all the winners
- Strict backup choice may be OK

NIST

Intellectual Property Study

- NIST IP Study
  - Are there potential infringement issues for the five finalists?
- Patent Search in U.S. & Europe
- Detailed infringement study of any “red flags”
- Results will be publicly available

NIST

Hardware

- FPGA vs. ASIC
  - do FPGAs matter?
    - ASICs may dominate if volume large
    - hard to do MARS FPGA
- Pipelining
  - doesn't work for feedback modes
  - need counter mode
- Parallel implementation
  - perhaps need new interleaved CBC modes

Key Agility

- Bigger concern for hardware
  - software implementations often can store many key schedules
- IPSec and Asynchronous Transfer Mode need key agility
  - many short messages with different keys
  - may be the most demanding application

NIST

Modes of Operation

- Conference on AES modes of operation suggested
- Counter mode
  – for pipelined performance
- Interleaved chaining or feedback modes
  – parallelism
- Superencryption?
  – alternative to backup?

Future AES Development Activities

May 15, 2000 - End of Round 2 comment period

Early Fall 2000 - Selection of AES algorithm(s)

Summer/Fall 2000 - Draft AES FIPS
Modes of Operation workshop
adopt DES modes for AES

Summer 2001 - Publish AES Standard
begin conformance testing,
draft Modes of Operation

NIST

Official Public Comments

- Official comments may be sent to

AESround2@nist.gov

Further Information

AES Home Page:

http://www.nist.gov/aes

NIST Points of Contact

- **Jim Foti** **<jfoti@nist.gov>**
- **Elaine Barker** **<ebarker@nist.gov>**
- **Ed Roback** **<eroback@nist.gov>**
- **Bill Burr** **<william.burr@nist.gov>**